RSA Archer® Exchange

RSA Archer® Suite

Version 6.8

Integration Guide

Revised: November 2020

RiskLens®

RSA ARCHER® SUITE

Contact Information
RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks
RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement
This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses
This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies
This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution
Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Revised: November 2020

Table of Contents

Release Notes

Fixed Issues

The following table describes fixed issues.

Date	Component	Description
November 2020	JavaScript Code	The Javascript code was failing when a RiskLens client secret value contains the '+' operator. This issue was fixed in the Javascript code. The verifyCerts data feed parameter option now has separate versions for Archer and RiskLens: - archerVerifyCerts for the Archer APIs - risklensVerifyCerts for the RiskLens APIs
September 2020	JavaScript Code	For customers who have RSA Archer configured to use HTTPS and have a self-signed SSL certificate or another form of non-perfected SSL certificate from a top tier Certificate Authority, data feeds were failing due to validation errors. To resolve this issue, the JavaScript code was updated. If you have RSA Archer configured to use HTTPS and have a self-signed SSL certificate or non-perfected SSL certificate, verify that the verifyCerts parameter in the RiskLens data feed is set to 'false'.

Chapter 1: Overview of RiskLens - RSA Archer® Integration

About RiskLens Cyber Risk Quantification

RiskLens is an enterprise-ready, Software as a Service (SaaS) platform that enables Security and Risk teams to quantify cyber risk from the business perspective.

Purpose-built on the Factor Analysis of Information Risk (FAIR) model, the only standard quantitative model for cybersecurity and technology risk, the RiskLens Platform integrates advanced quantitative risk analytics, best-practice risk assessment and reporting workflows; industry-specific loss data, and data from your security ecosystem, into a unified suite of applications built specifically for business-oriented CISOs and CIROs.

RiskLens uses Monte Carlo simulations in combination with the FAIR model. The platform allows the aggregation of multiple risk scenarios as well as the calculation of individual scenario results.

About RiskLens - RSA Archer Integration

The RiskLens and RSA Archer integration connects Risk Register records in the RSA Archer Platform to the RiskLens Cyber Risk Quantification Analysis, which allows the risks to be assessed with other factors that are based on FAIR quantified outputs. This integration allows for the creation of risk assessments in RiskLens from Risk Register. The integration updates the results in the corresponding Risk Register records with every analysis performed over time in RiskLens.

Key Features and Benefits

With the RiskLens integration, you can:

- Automatically create risk assessments in RiskLens for the Archer Risk Register records.
- Get the assessment analysis results from RiskLens to the Archer Risk Register records.
- Experience seamless integration with RiskLens based upon the data feed schedule.
- Keep your Risk Register up to date with latest RiskLens Cyber Risk quantification analysis results.

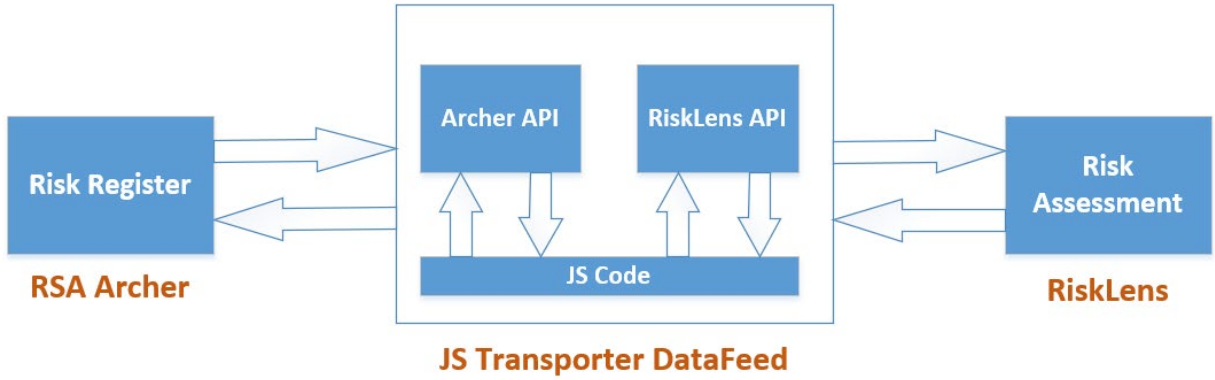
Requirements

Components	Requirement
RSA Archer Solution	• IT & Security Risk Management • Enterprise & Operational Risk Management
RSA Archer Use Case(s)	One or more of the following: • RSA Archer IT Risk Management • RSA Archer Information Security Management Systems • RSA Archer Top-Down Risk Assessment • RSA Archer Operational Risk Management

RSA Archer Applications	Leverages the Risk Register application
Uses Custom Application	No
Requires On-Demand License	No
RSA Archer Requirements	RSA Archer release 6.8 or later
RiskLens Requirements	RiskLens Gen3 and valid RiskLens license are required

Integration Diagram

The following diagram provides an overview of interaction between RSA Archer and RiskLens.



The following describes how data feeds work in the integration process:

1. The RSA Archer data feed for the RiskLens integration pulls the RSA Archer Risk Register record data from the source report “DFM_RiskLens” and creates risk assessments in RiskLens for each Risk Register record.

   When the risk assessment creation is completed in RiskLens, the data feed updates the respective Risk Register records in RSA Archer with Subscription ID and RiskLens Assessment URL field values.

2. The data feed pulls the risk assessment analysis results from RiskLens and updates the respective Risk Register records in RSA Archer with latest analysis results every time.

Chapter 2: Configuring the RiskLens - RSA Archer Integration

Before You Begin

This section provides instructions for configuring the RiskLens with the RSA Archer Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators must have access to the product documentation for all products in order to install the required components.

All RiskLens components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Important: The integration described in this guide is provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs of and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Configuring RiskLens

Create API Client

The API Client ID and Secret are used to configure the data feed in RSA Archer.

1. Log in to RiskLens.
2. Go to Administration.
3. On the API tab, click New API Client.
4. Copy the automatically populated Client ID and Secret.

   Note: The Secret field is only visible during creation of API Client. After API Client creation, RiskLens masks the Secret field in bullet format.
5. Enter a name.
6. Click Save.

Get RiskLens API URL

The RiskLens API URL is different from the RiskLens URL that you use to log in to RiskLens. For more information, contact your RSA Account Manager. For example: https://rsav3-api.risklens.com or https://v3-api.risklens.com

This API URL is used to configure the data feed in RSA Archer.

RiskLens APIs Used in Integration

The following are the RiskLens APIs used in this integration:

- Authentication: [RiskLens URL]/auth/connect/token
- Create Risk Assessment: [RiskLens API URL]/subscriptions/riskassessments
- Get Risk Analysis Results: [RiskLens API URL]/subscriptions

Configuring RSA Archer

Before you import the RiskLens data feed, complete the following tasks. Install any of the following use case packages, version 6.8 or later. These use cases contain the Risk Register application with RiskLens support changes:

- RSA Archer IT Risk Management
- RSA Archer Information Security Management Systems
- RSA Archer Top-Down Risk Assessment
- RSA Archer Operational Risk Management

After package installation, import the RiskLens data feed from the integration file.

Installing the Package

The following tasks detail how to import and install the use case package.

Task 1: Back up Your Database

There is no Undo function for package installation. Packaging is a powerful feature that can make significant changes to an instance. RSA strongly recommends backing up the instance database before installing a package. This process enables a full restoration if necessary.

Another option is to create a package of the affected objects in the target instance before installing the new package. This package provides a snapshot of the instance before the new package is installed, which can be used to help undo the changes made by the package installation. You must manually delete new objects created by the package

Task 2: Import the Package

1. Go to the Install Packages page.
    a. From the menu bar, click  .
    b. Under Application Builder, click Install Packages.
2. In the Available Packages section, click Import.
3. Click Add New, then locate and select the package file that you want to import.
4. Click OK.
   The package file is displayed in the Available Packages section and is ready for installation.

Task 3: Map Objects in the Package

1. In the Available Packages section, select the package you want to map.
2. In the Actions column, click  for that package.
   The analyzer automatically matches the system IDs of the objects in the package with the objects in the target instances. The analyzer also identifies objects from the package that are

successfully mapped to objects in the target instance, objects that are new or existing but are not mapped, and objects that do not exist (the object is in the target but not in the source).

Note: This process can take several minutes or more, especially if the package is large, and may time out after 60 minutes. The time-out setting temporarily overrides any IIS time-out settings set to less than 60 minutes.

When the analyzer completes, the Advanced Package Mapping page lists the objects in the package file and corresponding objects in the target instance. The objects are divided into tabs, depending on whether they are found within Applications, Solutions, Access Roles, Groups, Sub-forms, or Questionnaires.

3. On each tab of the Advanced Mapping Page, review the icons that are displayed next to each object name to determine which objects require you to map them manually.

The following table describes the icons.

Icon	Name	Description
	Awaiting Mapping Review	Indicates that the system could not automatically match the object or children of the object to a corresponding object in the target instance. Objects marked with this symbol must be mapped manually through the mapping process. **Important:** New objects should not be mapped. This icon should remain visible. The mapping process can proceed without mapping all the objects. **Note:** You can execute the mapping process without mapping all the objects. The  icon is for informational purposes only.
	Mapping Completed	Indicates that the object and all child objects are mapped to an object in the target instance. Nothing more needs to be done with these objects in Advanced Package Mapping.
	Do Not Map	Indicates that the object does not exist in the target instance or the object was not mapped through the Do Not Map option. These objects will not be mapped through Advanced Package Mapping and must be remedied manually.
	Undo	Indicates that a mapped object can be unmapped. This icon is displayed in the Actions column of a mapped object or object flagged as Do Not Map.

4. For each object that requires remediation, do one of the following:
    - To map each item individually, do the following:

a. On the Target column, select the object in the target instance to which you want to map the source object.
b. If an object is new or if you do not want to map an object, select Do Not Map from the drop-down list.

Important: Ensure that you map all objects to their lowest level. When objects have child or related objects, a drill-down link is provided on the parent object. Child objects must be mapped before parent objects are mapped. For more details, see "Parent and Child Object Mapping" in the RSA Archer Online Documentation.

- To automatically map all objects in a tab that have different system IDs but the same object name as an object in the target instance, do the following:
  a. In the toolbar, click Auto Map.
  b. Select an option for mapping objects by name.

  The following table describes the mapping options.

Option	Description
Ignore case	Matches objects with similar names regardless of the case of the characters in the object names.
Ignore spaces	Matches objects with similar names regardless of whether spaces exist in the object names.

  c. Click OK.

  The Confirmation dialog box opens with the total number of mappings performed. These mappings are not committed to the database yet and can be modified on the Advanced Package Mapping page.

  d. Click OK.
- To set all objects in the tab to Do Not Map, in the toolbar, click Do Not Map.

  Note: To undo the mapping settings for any individual object, click  in the Actions column.

When all objects are mapped, the  icon is displayed in the tab title. The  icon is displayed next to the object to indicate that the object will not be mapped.

5. Verify that all other objects are mapped correctly.
6. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in the RSA Archer Online Documentation.
7. After you have reviewed and mapped all objects, click  .
8. Select “I understand the implications of performing this operation” and click OK.

The Advanced Package Mapping process updates the system IDs of the objects in the target instance as defined on the Advanced Package Mapping page. When the mapping is complete, the Import and Install Packages page is displayed.

Important: Advanced Package Mapping modifies the system IDs in the target instance. Any Data Feeds and Web Service APIs that use these objects will need to be updated with the new system IDs.

Task 4: Install the Package

All objects from the source instance are installed in the target instance unless the object cannot be found or is flagged to not be installed in the target instance. A list of conditions that may cause objects not to be installed is provided in the Log Messages section. A log entry is displayed in the Package Installation Log section.

1. Go to the Install Packages page.
    a. From the menu bar, click  .
    b. Under Application Builder, click Install Packages.
2. In the Available Packages section, do the following:
    a. Locate the package file you want to install.
    b. In the Actions column, click  .
3. In the Selected Components section, select the components of the package that you want to install.
    - To select all components, select the top-level checkbox.
    - To install only specific global reports in an already installed application, select the checkbox associated with each report that you want to install.

    Note: Items in the package that do not match an existing item in the target instance are selected by default.
4. Click Lookup.
5. For each component section, do the following:
    Note: To move onto another component section, click Continue or select a component section in the Jump To drop-down menu.
    a. In the Install Method drop-down menu, select an install method for each selected component.
    Note: If you have any existing components that you do not want to modify, select Create New Only. You may have to modify those components after installing the package to use the changes made by the package.
    b. In the Install Option drop-down menu, select an install option for each selected component.
    Note: If you have any custom fields or formatting in a component that you do not want to lose, select Do Not Override Layout. You may have to modify the layout after installing the package to use the changes made by the package.

6. Click OK.
7. To deactivate target fields and data-driven events that are not in the package, in the Post-Install Actions section, select the Deactivate target fields and data-driven events that are not in the package checkbox. To rename the deactivated target fields and data-driven events with a user-defined prefix, select the Apply a prefix to all deactivated objects checkbox, and enter a prefix. This can help you identify any fields or data-driven events that you may want to review for cleanup post-install.
8. Click Install.
9. Click OK.

Task 5: Review the Package Installation Log

1. Go to the Package Installation Log tab of the Install Packages page.
    a. From the menu bar, click  .
    b. Under Application Builder, click Install Packages.
    c. Click the Package Installation Log tab.
2. Click the package that you want to view.
3. In the Package Installation Log page, in the Object Details section, click View All Errors.

For a list of packaging installation log messages and remediation information for common messages, see "Package Installation Log Messages" in the RSA Archer Online Documentation.

Configure the Data Feed

RiskLens Data Feed is a JavaScript transporter data feed that:

- Creates risk assessments in RiskLens for each Risk Register record of RSA Archer.
- Retrieves the assessment analysis results and updates the records in the RSA Archer Risk Register application.

After setting up the data feed, you must configure the data feed. You can schedule data feeds to run as needed per the requirements for your organization. For more information on Scheduling Data Feeds, see Scheduling Data Feeds.

Configure the JavaScript Transporter Settings

Before you upload a JavaScript file, you must configure JavaScript Transporter settings in the RSA Archer Control Panel.

1. On the general tab, go to the JavaScript Transporter section.
    a. Open the RSA Archer Control Panel.
    b. Go to Instance Management and select All Instances.
    c. Select the instance you want to use.
    d. On the General Tab, go to the JavaScript Transporter section.
2. In the Max Memory Limit field, set the value to 2048 MB (2 GB).
3. In the Script Timeout field, set the value to 120 minutes (2 hours).

4. (Optional) To allow only digitally signed JavaScript files in the data feed, enable the Require Signature option.
    a. In the JavaScript Transporter Settings section, select the Require Signature checkbox. A new empty cell appears in the Signing Certificate Thumbprints section.
    b. In the Signing Certificate Thumbprints section, double-click an empty cell.
    c. Enter the digital thumbprint of the trusted certificate used to sign the JavaScript file.
    Note: For information on how to obtain digital thumbprints, see Obtaining Digital Thumbprints.
    Important: If you enable Require Signature and specify no thumbprints, no JavaScript files will be accepted by the system.
    d. (Optional) If you want to add additional thumbprint sources, repeat steps b-c for each thumbprint.
5. On the tollbar, click Save.

Obtaining Digital Thumbprints

When running JavaScript data feeds, you can set the system to only allow digitally signed JavaScript files from trusted sources for security considerations.

For a certificate to be trusted, all the certificates in the chain, including the Root CA Certificate and Intermediate CA certificates, must be trusted on both the Web Server and Services Server machines.

RSA Security LLC Cert in the Trusted Root CA Store

RSA Security LLC certificate is not present on every machine's root by default.

1. On the JavaScript file, right-click and select Properties.
2. Click the Digital Signatures tab.
3. From the Signature List window, select RSA Security LLC.
4. Click the Details button.
5. Click View Certificate.
6. Click Install Certificate.
7. Select Local Machine.
8. Click Next.
9. Select Place all certificates in the following store and click Browse.
    a. Select Trusted Root Certification Authorities and click OK.
    b. Click Next.
    c. Click Finish.
10. Upon successful import, click OK.

Obtain a Certificate Thumbprint

1. In the RSA Archer Control Panel environment, open the Manage Computer Certificates program.
    a. Click Start.
    b. Type: certificate.
    c. From the search results, click Manage Computer Certificates.
2. Ensure that your trusted source certificates are in the Certificates sub-folder of the Trust Root Certification Authorities folder.
3. In the Certificates sub-folder, double-click the RSA Security LLC certificate that contains the thumbprint you want to obtain.

4. Verify that the certificate is trusted.
    a. In the Certificate window, click the Certification Path tab.
    b. Ensure that the Certificate Status windows displays the following message:
    c. THIS certificate is OK

    Note: If the Certificate Status windows displays something different, follow the on-screen instructions.
5. Obtain the trusted certificate thumbprint.
    a. In the Certificate window, click the Details tab.
    b. Select the Thumbprint field. The certificate's digital thumbprint appears in the window.
    c. Copy the thumbprint.

Set up the RiskLens Data Feed

Important: Before you upload a JavaScript file, configure JavaScript Transporter settings in the RSA Archer Control Panel. For more information, see Configure the JavaScript Transporter Settings.

1. Go to the Manage Data Feeds page.
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the RiskLens_Data_Feed.dfx5 file.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. Click the Transport tab.
7. In the Transport Configuration section, do the following:
    a. Click Upload.
    b. From the Upload JavaScript File dialog, click Add New.
    c. Locate and select the RiskLens.js file.
    d. Click Open.
    e. From the Upload JavaScript File dialog, click OK.
8. In the Custom Parameters section, enter key values.

    The following table describes the value for each key in Custom Parameters.

Key	Value
archerUrl	[Valid value] Default = [empty] (**Required**)
archerInstance	[Valid value] Default = [empty] (**Required**)
archerUser	[Valid value] Default = [empty] (**Required**)
archerPass	[Valid value]

	Default = [empty] (**Required**)
risklensUrl	[Valid value] Default = https://rsav3.risklens.com* (**Required**)
risklensApiUrl	[Valid value] Default = https://rsav3-api.risklens.com* (**Required**)
risklensClientID	[Valid value] Default = [empty] (**Required**)
risklensClientSecret	[Valid value] Default = [empty] (**Required**)
proxy	[Valid value] Default = [empty] (Optional)

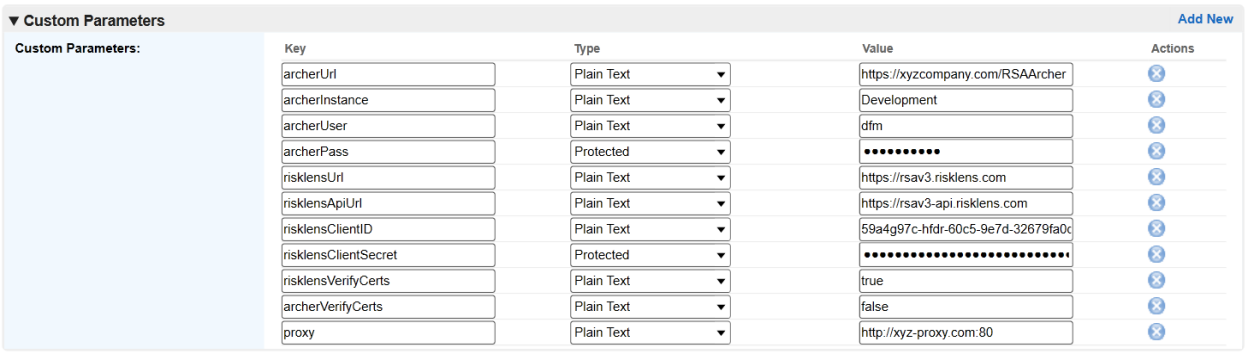
*Update the default value if your risklens url is different.

9. The following additional parameters provide RiskLens and Archer API validation in the Custom Parameters section for the current JavaScript file.

risklensVerifyCerts	[Valid value of true/false] Default = true (Required)
archerVerifyCerts	[Valid value of true/false] Default = false (Required)

If verifyCerts = true, the node JS validates whether the endpoint certificate is from a trusted Certificate Authority (CA). The related API requests succeed if the endpoint certificate is from a trusted CA.

The following is an example of the data feed custom parameters values:



Scheduling Data Feeds

When you schedule a data feed, the Data Feed Manager validates the information. If any information is invalid, an error message will display. You can save the data feed and correct the errors later, but the data feed is not processed until the errors are rectified.

Important: A data feed must be active and valid to successfully run.

1. Go to the Schedule tab of the data feed that you want to modify.
   a. From the menu bar, click  .
   b. Under Integration, click Data Feeds.
   c. Select the data feed you want to modify.
   d. Click the Schedule tab.
2. Complete the Recurrences section.
   The following table describes the fields in the Recurrences section.

Field	Description
Frequency	Specifies the interval in which the data feed runs. • **By minute:** Runs the data feed by the minute interval set. For example, if you specify 45 in every list, the data feed executes every 45 minutes. • **Hourly:** Runs the data feed by the hourly interval set. For example, every hour (1), every other hour (2), and so forth. • **Daily:** Runs the data feed by the daily internal set. For example, every day (1), every other day (2), and so forth. • **Weekly:** Runs the data feed based on a specified day of the week. For example, every Monday of the first week (1), every other Monday (2), and so forth. • **Monthly:** Runs the data feed based on a specified week of the month. For example, 1st, 2nd, 3rd, 4th, or Last. • **Reference:** Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. From the Reference Feed list, select after which existing data feed the current data feed starts. A reference data feed will not run when immediately running a data feed. The Data Feed Now option only runs the current data feed.
Every	Specifies the interval of the frequency in which the data feed runs.
Start Time	Specifies the time the data feed begins running.
Start Date	Specifies the date on which the data feed schedule begins.
Time Zone	Specifies the time zone in of the server that runs the data feed.

3. (Optional) In the Run Data Feed Now section, click Start to override the data feed schedule and run the data feed immediately.
4. Click Save.

Upgrade Notes and Procedures for Risk Register

The following steps are only required for upgrading customers.

Update the Assessment Method Field

In Risk Register, the RiskLens Quantitative Analysis value is now in the Assessment Method field. This field selection is required when the Assessment Approach field selection is Quantitative Survey. After completing the Package Installation, upgrading customers must set the Assessment Approach as Quantitative Survey and the Assessment Method as RiskLens Quantitative Analysis in all existing Risk Register RiskLens Quantitative Analysis records.

You can update your existing records through Bulk Schedules, Bulk Update, or a Data Import. To update records through a bulk schedule, use the following steps:

1. Create a new Bulk Schedule. Do the following:
    a. Enter a name for the schedule.
    b. Set the status to Active.
    c. Select the application: Risk Register.
    d. Add the filter: [Assessment Approach] Equals RiskLens Quantitative Analysis
2. Save the schedule.
3. Add a new Bulk Action. Do the following:
    a. Enter a name for the action.
    b. In the Type field, select Bulk Update.
    c. In the Field Value Expression section:
        i. Select [Assessment Approach] and corresponding value as Quantitative Survey.
        ii. Select [Assessment Method] and corresponding value as RiskLens Quantitative Analysis.
4. Save the Bulk Action and Bulk Schedule.
5. Run the Bulk Schedule.
6. When all records have been updated, you may delete or inactive the Bulk Schedule.
7. Inactivate or delete the value “RiskLens Quantitative Analysis” value from Assessment Approach field.

Inactivate or Delete Fields and DDEs

The following fields no longer support RiskLens Gen3 version integration and are deleted from the latest version of Risk Register:

- Analysis Complete Date
- Analysis Request Date
- Request Status
- RiskLens Request Status
- Adjusted RiskLens Residual Risk

After package installation, the DDEs that were not updated through the package installation can be inactivated or deleted.

Chapter 3: Using the RiskLens - RSA Archer Integration

Create a Risk Assessment in RiskLens from Risk Register

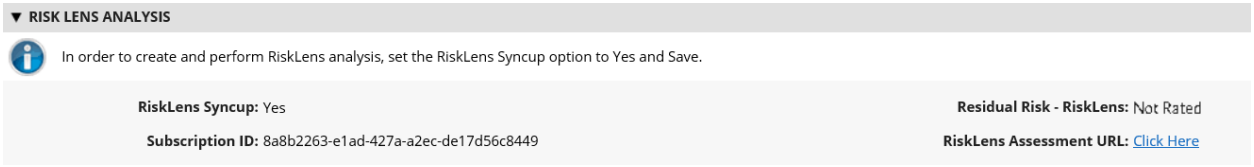
User: Archer End User

1. Populate the Risk Register record with your risk.
2. Select the Assessment Approach field value as Quantitative Survey.
3. In Assessment Method field, select RiskLens Quantitative Analysis.
   The Qualitative Survey and RiskLens Analysis sections display in the Risk Analysis tab.
4. In the Status field, select Active.
   Note: Inherent and Residual Risk does not calculate until the status is set to Active.
5. Complete the Qualitative Survey section.
6. Click Save.
   The Inherent Risk gets populated.
7. In the RiskLens Analysis section, in the RiskLens Syncup field, select Yes.
8. Click Save.
   The scheduled data feed creates the Risk Assessment in RiskLens and updates the related RSA Archer Risk Register record with the Subscription ID and RiskLens Assessment URL.

The RiskLens risk assessment sets the Name as a combination of the Archer Risk ID and Risk Name. The Purpose is set as the Archer Risk Description.

Note: The RiskLens risk assessment accepts 200 characters in the Name field and 1,000 characters in the Purpose field. Risk Register record data that exceeds the character limit is truncated in the RiskLens fields.

After RiskLens creates the risk assessment, the risk register record updates as follows:



Generate RiskLens Analysis Results for the Risk Register Record

User: Archer End User

After the data feed creates the risk assessment, perform the following steps in RiskLens.

1. For the RiskLens risk assessment, create the needed scenarios with the relevant assets.
2. Run the analysis.
3. In the ellipses menu, select the Set as Current option for the analysis results.
   The scheduled data feed updates the Archer Risk Register record with the latest RiskLens analysis

results.

Note: The RiskLens Syncup field in the Risk Register record must be set to Yes for the scheduled data feed to work.

In the Risk Register record, the calculated Residual Risk from RiskLens is based on the Loss Exposure 90th value.

Capturing Errors

If any of the records fail to create the risk assessment or get analysis results, the failure reason is captured in the RiskLens Integration Error field.

If all the records in the source report fail to process, the data feed is faulted.

Load Capacity

The data feed in RSA Archer supports up to 2,000 records in a run. The load capacity has been tested with 1,000 Create Assessment records and 1,000 Get Analysis records. A higher load capacity can be configured but has not been tested for performance and stability.

Additional Information

1. Risk Register creates the Loss Exposure 10th and Loss Exposure 90th values by considering the default RiskLens percentile values as 10 and 90. If your organization follows different lower and higher percentile values in RiskLens, you can rename the Loss Exposure 10th and Loss Exposure 90th fields in Risk Register to match your configured percentile values.
2. The data feed updates RiskLens analysis results in a Risk Register record only if there is a new analysis result. The data feed does not consider the risk register record to update analysis results if there is no new result.

Appendix A: Certification Environment

Date Tested: November 2020

Product Name	Version Information	Operating System
RSA Archer Suite	6.8 and later	Virtual Appliance
RiskLens	RL 3.6.0	Virtual Appliance